**WHAT IS CLAIMED IS:**

Claim 1. A method for authenticating a user in a process-based security system, comprising the steps of:

sending an initiation request from an authenticating process to an authentication module;

modifying a task structure of the authenticating process to indicate the initiation request;

generating a random number at said authentication module;

sending said random number to said authenticating process;

performing a transformative function on said random number and a user password by the authenticating process to form first authenticating data;

sending said first authenticating data and user identification data to said authentication module;

retrieving a user password associated with the received user identification data by the authentication module;

performing said transformative function on said random number and said retrieved user password by the authentication module to form second authenticating data;

comparing said first authenticating data with said second authenticating data, such that when said first authenticating data is equal to said second authenticating data, the user identified by the user identification data is authenticated.

Claim 2. The method of authenticating in accordance with claim 1, wherein said authenticating process is a login routine.

Claim 3. The method of authenticating in accordance with claim 1, wherein said authentication module is part of an operating system.

Claim 4. The method for authenticating of claim 1, further comprising the step of checking the task structure of the authenticating process to determine if an authentication has been initiated before the step of retrieving a user password.

Claim 5. The method for authenticating of claim 1, wherein said transformative function in a hash function.

Claim 6. The method for authenticating of claim 1, wherein said transformative function is a keyed MD5 signature function.

Claim 7. The method for authenticating of claim 1, wherein said random number is a cryptographically strong pseudo-random number.

Claim 8. The method for authenticating of claim 1, further comprising the step of storing the user password in unencrypted form.

Claim 9. The method for authenticating of claim 1, wherein said transformative function is performed on said random number concatenated with said user password.

Claim 10. The method for authenticating of claim 1, further comprising the step of modifying the task structure of the authenticating process to indicate completion of the initiation request.

Claim 11. A system for authenticating a user in a process-based security system, comprising:

an authentication module;

an authenticating process in communication with said authentication module;

wherein said authenticating process sends an authentication request to an authentication module and the authentication modifies a task structure of the

authenticating process to indicate the authentication request; wherein the authentication module generates a random number and send said random number to said authenticating process, the authenticating process performing a transformative function on said random number and a user password to form first authenticating data; the authenticating process sends said first authenticating data and user identification data to said authentication module; the authentication module retrieves a user password associated with the received user identification data and performs said transformative function on said random number and said retrieved user password to form second authenticating data; and

the authentication module compares said first authenticating data with said second authenticating data, such that when said first authenticating data is equal to said second authenticating data, the user identified by the user identification data is authenticated.

Claim 12. The system for authenticating in accordance with claim 11, wherein said authenticating process is a login routine.

Claim 13. The system for authenticating in accordance with claim 11, wherein said authentication module is part of an operating system.

Claim 14. The system for authenticating of claim 11, further comprising the authentication module checking the task structure of the authenticating process to determine if an authentication has been initiated before the step of retrieving a user password.

Claim 15. The system for authenticating of claim 11, wherein said transformative function in a hash function.

Claim 16. The system for authenticating of claim 11, wherein said transformative function is a keyed MD5 signature function.

Claim 17. The system for authenticating of claim 11, wherein said random number is a cryptographically strong pseudo-random number.

Claim 18. The system for authenticating of claim 11, further comprising the step of storing the user password in unencrypted form.

Claim 19. The system for authenticating of claim 11, wherein said transformative function is performed on said random number concatenated with said user password.

Claim 20. The system for authenticating of claim 11, further comprising the authentication module modifying the task structure of the authenticating process to indicate completion of the initiation request.